~~SPECIFICATION~~

~~METHOD AND COMMUNICATIONS SYSTEM FOR CIPHERING INFORMATION FOR A RADIO TRANSMISSION AND FOR AUTHENTICATING OF SUBSCRIBERS~~

The invention is directed to a method for the encryption of information for a radio transmission and for authentication of subscribers in a communication system and is also directed to a corresponding communication system.

Description of the Related Art

Communication systems such as, ~~for example,~~ the mobile radio telephone system according to the GSM standard (global system for mobile communication) use a radio interface for wireless information transmission between mobile stations and base stations of a mobile radio telephone network. ~~being capable of being~~ setup, released and maintained on ~~said~~ radio interface. A method and a system for encryption (ciphering) information for radio transmission and for subscriber authentication are known from the article "Safety First bei europaweiter Mobilkommunikation", telcom report 16 (1993), No. 6, pages 326 through 329. ~~The~~ mobile subscribers ~~thereby~~ identify themselves with respect to the mobile radio telephone network using a ~~means - also referred to as~~ subscriber identity mobile ~~or~~ (SIM) card, that is contained in the radio telephone subscriber station. At the network side, the mobile subscriber is registered in a ~~means - for example,~~ an authentication means (authentication center), that respectively offers security parameters and security algorithms for the protection of the subscriber data of the mobile subscribers. The encryption of the information on the radio interface ~~ensues~~ takes place in a subscriber-related manner and is directly coupled to the subscriber authentication.

In future communication systems, such as, ~~for example,~~ a universal network (UMTS, universal mobile telecommunication system or UPT, universal personal communication), there is ~~the~~ a tendency to divide the infrastructure into an access network and into one or more core networks.

The area of the access network ~~is thereby~~ responsible for matters of the radio interface such as administration and allocation of the radio channels, channel encoding, encryption via the radio interface, ~~etc., in contrast whereto~~ the area of the core network is mainly responsible for matters of the subscriber administration such as registration (subscription), authentication, selection of the access network, etc., as well as for offering services. An encryption of the information for the radio transmission independently of the core network is impossible in the current GSM system. Over and above this, a radio resource, for example the radio channel, is exclusively used for only one subscriber in the encryption, namely the subscriber that was authenticated at the moment, ~~this~~ no longer ~~being~~ adequate ~~in~~ future communication systems, particularly given simultaneous use of a mobile station by a plurality of subscribers (for example, with their SIM cards).

The invention is based on the object of specifying a method and a communication system that enables an encryption of the information at the radio interface independently of the nature and plurality of core networks, ~~so that~~ a functional separation of encryption and authentication ~~derives~~.

~~This object is inventively achieved by the method comprising the features of patent claim 1 and by the communication system comprising the features of patent claim 12. Developments of the invention can be derived from the subclaims.~~

The subject matter of the invention proceeds from an encryption of the information for the radio transmission in an access network as well as from an authentication in at least one core network. Inventively, public keys are transmitted in alternation between a mobile station that can be used in parallel by a plurality of subscribers and the base station, being sent via the radio interface, and the public key received by the base station or, ~~respectively,~~ mobile station is employed for the encryption of the information to be subsequently transmitted via the radio interface. The encrypted information received by the mobile station or, ~~respectively,~~ base station can be deciphered on the basis of a private key that is allocated in the mobile station or, ~~respectively,~~ in the base station to the public key that was

transmitted. Following the deciphering procedure, the authentication of the respective core network is implemented by a ~~means~~ component/equipment of the mobile station, and the authentication of the subscriber is implemented by ~~the means~~ a component/equipment of the core network on the basis of the encrypted information transmitted in alternation.

As a result of the mutual transmission of public keys between mobile station and base station, the encryption for the radio transmission can ~~ensue~~ take place in mobile station-related manner instead of a subscriber-related manner and, thus, can simultaneously ensue for a plurality of subscribers. There is a bidirectional, trusted relationship into which an "apparent" base station or an unauthorized base station cannot intervene. Another advantage is the functional separation of access network (responsible for encryption) and core network (responsible for authentication). The radio resource is multiply utilized for the encryption of a plurality of subscribers at the mobile station. The information required for the authentication procedure can already be transmitted encrypted, ~~this having not been~~ which was not possible in the previous GSM system. Maximum security is achieved by the combination of the encryption with public/private keys at the mobile station level and the following authentication at the subscriber level. In particular, a plurality of core networks - potentially of different network types - can be connected parallel to the access network due to the functional separation of access network and core network, and, in particular, a plurality of subscribers having different identities (SIM cards) can communicate simultaneously via a mobile station and in different core networks.

No third party can subsequently sneak into the secure connection, achieved by multiple, mutual transmission of the public keys. The following authentication assures that the respective partner ~~means~~ device of the connection - i.e., the base station from the point of view of the mobile station or, respectively, the mobile station from the point of view of the base station - is also in fact the ~~means~~ device that it pretended to be at the beginning of the communication.

An advantageous development of the invention provides that the mobile station first sends a first public key to the base station, ~~that latter using this~~ which uses this key for the encryption of the information, and a public key is sent from the base station to the mobile station that employs it for the encryption of the information. Subsequently, the mobile station sends a second public key to the base station. The involvement of an "apparent" base station or of the unauthorized base station into the connection is thus dependably prevented at the radio interface. The second key thereby preferably replaces the first key.

According to an alternative development of the invention, the base station first sends a first public key to the mobile station, which employs it for encryption of the information, and the mobile station sends a public key to the base station, which employs it for the encryption of the information. Subsequently, the base station sends a second public key to the mobile station. The involvement of the "apparent" base station or of the unauthorized base station in the connection is thus dependably prevented at the radio interface. The second key is thereby preferably replaced by the first key.

It is advantageous according to another development of the invention that the mobile station sends a subscriber identity of the subscriber and an authentication request to the core network in encrypted form and receives an authentication reply from the ~~means of the~~ core network sent back to it in encrypted form. Subsequently, the mobile station implements an authentication procedure for checking the identity of the core network. A network authentication thus ~~ensues~~ occurs at the side of the mobile station, ~~this being capable of being~~ which can be individually implemented, particularly ~~given~~ for a plurality of core networks dependent on where the subscriber is registered.

The ~~means of the~~ core network preferably sends an authentication request in addition to the authentication reply in encrypted fashion, and an authentication reply is sent back to the ~~means from the~~ mobile station in encrypted form. Subsequently, ~~the means of~~ the core network can implement an authentication procedure for checking the subscriber identity.

This has the advantage that the request for checking the subscriber authentication can be co-transmitted with the reply of the network ~~means~~ to the network authentication and can be initiated by the network ~~means~~ immediately upon arrival of the reply.

A communication system according to the invention comprises memory ~~means~~ as a mobile station that can be used in parallel by a plurality of subscribers and of the base station for storing public keys and private keys that are allocated to the public keys. Transmission devices in the mobile station and in the base station ~~see to~~ the mutual transmission of the public keys via the radio interface. Control devices in the mobile station and in the base station are provided for the encryption of the information to be subsequently transmitted via the radio interface upon employment of the public key received from the base station or ~~respectively~~, mobile station and for deciphering the received, encrypted information on the basis of the stored, appertaining private key. Over and above this, the communication system comprises a subscriber-specific ~~means~~ in the mobile station and a ~~control means~~ in the respective core network for the implementation of the authentication of the core network as well as of the authentication of the subscribers on the basis of mutually transmitted, encrypted information.

The invention is explained in greater detail below on the basis of an exemplary embodiment with reference to the graphic illustration.

~~Thereby shown are:~~

FIG. 1 ~~the~~ block circuit diagram of a communication system with an access network for the radio transmission and a plurality of core networks for the authentication;

FIG. 2 ~~the~~ message flow for the encryption of the information at the radio interface between a mobile station and a base station of the access network; and

FIG. 3 ~~the~~ message flow for the authentication of the subscribers and of the core networks between the mobile station and ~~a network means of~~ the respective core network.

The communication system show in FIG. 1 is a universal communication system UNW - such as, ~~for example,~~ a universal UMTS or UPT network (universal mobile telecommunication system or universal personal telecommunication) - whose infrastructure is divided into an access network ACN and into one or more core networks CON1, CON2. The area of the access network ACN having devices of a radio sub-system - such as, ~~for example,~~ base stations BS and base station controllers BSC connected ~~thereto - is thereby~~ to it - is responsible for matters of the radio interface such as administration and allocation of radio channels, channel encoding, encryption via the radio interface, etc. The area of the core network CON1, CON2 with network equipment - such as, ~~for example,~~ switching equipment MSC, MSC' and authentication equipment AC, AC' - is mainly responsible for matters of routing, of subscriber administration such as registration (subscription) of the subscribers S1, S2 as well as authentication, selection of the access network ACN, etc., and for offering services. The authentication procedures in the ~~means~~ authentication equipment AC, AC' preferably use secret keys ki according to the known procedure of the GSM standard in order to implement the subscriber authentication for the subscriber S1 registered in the core network CON1 and for the subscriber S2 registered in the core network CON2 in parallel and independently of the access network ACN.

In the present example, the switching equipment MSC, MSC' in the core networks CON1 and CON2 are connected to the base station controller BSC of the access network ACN. The base station controller BSC enables the connection to at least one base station, to the base station BS in the present example. Such a base station BS is a radio station that is provided for coverage of a radio area - for example, of a radio cell - in order to setup, release and maintain connections from/to at least one mobile station MT that resides in its radio area via radio interface AI. The information are ~~thereby~~ contained in a radio channel RCH allocated by the base station controller BSC. The connections can be a matter of outgoing connections as well as of incoming connections. The mobile station MT in the present example is especially suited for simultaneous use by a plurality of subscribers S1 and

S2 that are attached in parallel to an internal bus (not shown) on the basis of their subscriber-specific devices SIM (subscriber identity module) and each have respectively separate subscriber identity.

The mobile station MT comprises a memory ~~means~~ MSP, a ~~transmission and reception means~~ transmitter and receiver MSE as well as control devices MST, MST' that are connected to the memory means MSP and ~~transmission and reception~~ transmitter and receiver means MSE. Likewise, the base station BS comprises a memory ~~means~~ BSP, a ~~transmission and reception means~~ transmitter and receiver BSE as well as a ~~control means~~ controller BST that is connected to the memory ~~means~~ BSP and ~~transmission and reception means~~ transmitter and receiver BSE.

According to the invention, the mobile station MT ~~station-related via the transmission and reception means~~ MSE - sends a first public key PUK1-MT via the radio interface AI in parallel for all subscribers active at it and makes note of an appertaining, private key PRK1-MT that is deposited in the memory ~~means~~ MSP or in the ~~control means~~ controller MST. The base station BS employs the received, public key PUK1-MT for the encryption of the information to be subsequently sent via the radio interface AI. The deciphering of the information sent by the base station BS is thus only possible for the ~~means~~ entity that knows the appertaining private key, i.e., the mobile station MT with the key PRK1-MT. The base station It in turn sends a public PUK-BS in the reply of the base station BS in the opposite direction to the mobile station MT and makes note of the appertaining private key PRK1-BS. The memory ~~means~~ BSP or the ~~control means~~ controller BST stores the private key PRK1-BS. It is thus assured that information subsequently sent by the mobile station MT to the base station BS, ~~these being~~ which are encrypted upon employment of the public key PUK1-BS, can only in turn be deciphered by the base ~~station BS or, respectively, the control means BST thereof.~~ station BS or its controller BST

In order to prevent an "apparent" base station or unauthorized base station from using the public key PUK1-MT communicated from the mobile station MS for sending correctly encrypted information, arbitrarily or intentionally, the mobile station MT sends a second public key PUK2-MT (already encrypted) to the base station BS via the radio interface AI. This

key PUK2-MT can only be read and employed by the correct base station BS with which a trusted relationship was initially set up on the mobile station level. The "apparent" base station or unauthorized base station is dependably suppressed in this ~~[...]~~ method. The second public key PUK2-MT ~~thereby~~ thus replaces the previous, first public key PUK1-MT. The same is true ~~of~~ in the other transmission direction when the mutual transmission of the keys was initiated by the base station BS.

The encryption procedure can likewise be initiated by the base station BS, so that the ~~transmission and reception means~~ transmitter and receiver BSE sends a first public key PUK1-BS to the mobile station MT, ~~said first public key PUK1-BS having~~ which has a private key PRK1-BS allocated to it and ~~being~~ stored in the ~~control means~~ controller BST or in the memory ~~means~~ BSP. The mobile station MT employs the arriving, public key PUK1-BS for encryption of the ~~following~~ information that follows it and in turn sends a public key PUK-MT to the base station BS that employs it for the encryption of the information in the opposite direction. Subsequently, the base station BS preferably sends a second public key PUK2-BS to the mobile station MT in order to be absolutely certain that an undesired base station does not mix itself into the encrypted information transmission via the radio channel or ~~listen to this~~ eavesdrop. The public as well as the private keys are composed, for example, of a numerical sequence or bit sequence.

Following the encryption procedure, the mobile station MT - preferably, the ~~means~~ subscriber identity mobile card SIM provided only for the authentication, or a control means MST responsible in common for encryption and authentication - implements the authentication of the respective core network CON1, CON2, and the ~~means~~ authentication equipment AC, AC' of the core network CON1, CON2 implements the authentication of the subscriber S1, S2 on the basis of mutually transmitted, encrypted information at the subscriber level (see Fig. 3). The bidirectional authentication is thus implemented independently of the access network ACN. The authentication appended to the encryption offers maximum security since it assures that the cooperating ~~means~~ entity of the connection is in fact the ~~means~~ entity that it identified itself ~~as~~ at the beginning of the communication. This prevents the overall communication on this connection

from having been initiated by an "apparent" base station or unauthorized base station. Another advantage of the functional separation of encryption and authentication is ~~comprised thereof~~ that the subscriber identities and the information required for the authentication - for example, random number RAND, and signed response SRES according to a GSM method - can already be transmitted encrypted via the radio interface AI. Authentication procedures deviating from GSM methods can also be employed for the authentication.

A plurality of core networks, the two core networks CON1, CON2 in the present example, even if different network types, can be connected parallel to the access network ACN. The subscribers S1, S2 simultaneously work with different SIM cards via the one mobile station MT in different core networks - in the two core networks CON1, CON2 in the present example - or, respectively, one or more subscribers S1, S2 work in a single core network, for example CON1. Furthermore, ~~Further~~, the functional separation of the access network ACN and the core network CON1, CON2 also supports configurations in which ~~wherein~~ the access network ACN and the core network or networks CON1, CON2 exhibit different network operators.

In a schematic illustration, FIG. 2 shows the message flow for encryption of the information for the radio transmission between the mobile station MT and the base station BS of the access network. This ~~The~~ example is ~~thereby~~ limited ~~thereto~~ in that the mutual exchange of the keys is initiated by the mobile statio MT. The base station BS could likewise begin the exchange (also see the description for FIG. 1); the following message flow would then be executed in a corresponding way.

After the allocation of the radio channel RCH for a connection setup for communication, the mobile station MT starts the encryption in that it transmits the public key PUK1-MT in a message SEND and makes note of the appertaining, private key PRK1-MT. The encrypted transmission of the information has thus begun at the radio interface. The base station BS uses the arriving key PUK1-MT for encrypted information transmission in the opposite direction, and in turn transmits the public key PUK-BS in the message SEND. It also makes note of the private key PRK1-BS belonging

to the public key PUK-BS. The information transmitted in encrypted form - at least the public key PUK-BS in the present case - can only be deciphered by the mobile station MT with the assistance of the private key PRK1-MT that is only known to it. After the deciphering, the mobile station MT sends a second public key PUK-MT to the base station BS in a further message SEND, this base station BS deciphering the arriving information - at least the second public key PUK2-MT in the present case - with the assistance of the private key PRK1-BS that is only known to it. The second public key PUK2-MT thereby replaces the previous, first public key PUK1-MT. A trusted relationship has thus been produced between the two devices, and third parties are not ~~being~~ capable of penetrating ~~into~~ this relationship.

In a schematic illustration, FIG. 3 shows the message flow for authentication of the subscribers S1, S2 registered in different core networks and for authentication of the respective core network. Messages are ~~thereby~~ transmitted between the subscribers S1, S2 using the mobile station MT and the network equipment AC, AC' (authentication center) of the respective core network, and are ~~being~~ transmitted transparently for the access network and the base station ~~thereof~~ of it.

First, the subscriber S1 or, respectively, the mobile station MT transmits an authentication request aureq-mt via the subscriber ~~-specific means~~ identity mobile card (SIM) for the subscriber and a subscriber identity SID ~~-on the basis of the subscriber-related SIM card-~~ in the message SEND to the ~~means~~ authentication equipment AC of the core network responsible for the subscriber S1. The transmission of the information takes place in ~~thereby ensues~~ format encrypted. In the opposite direction, the ~~means~~ authentication equipment AC returns an authentication reply aures-co in the message SEND to the mobile station MT that implements the authentication procedure - with, preferably, a secret key - for checking the authentication for the core network. With the authentication reply aures-co, an authentication request aureq-co is preferably simultaneously co-transmitted from the ~~means~~ authentication equipment AC of the core network in encrypted form and is received by the mobile station MT. In response ~~thereto~~, the mobile station returns an authentication reply aures-mt in the message SEND to the ~~means~~ authentication equipment AC in encrypted form and subscriber-

related, ~~said means~~ AC ~~implementing~~ the authentication procedure for checking the subscriber authentication in a likewise, preferably, upon employment of secret keys. An authentication in only one direction - i.e., only for the subscribers or for the network - is also fundamentally possible.

The executive sequence for the authentication of the subscriber S2 takes place ~~ensues~~ in a corresponding way by exchanging messages SEND having the above contents between the corresponding, subscriber ~~-specific means (SIN)~~ identity mobile card (SIM) of the mobile station MT and the ~~network means~~ authentication equipment AC of the other core network responsible for it. As a result of the combination of encryption at the radio interface from/to the access network achieved on the basis of repeatedly exchanged public keys on the mobile station level, and following the authentication using secret keys on the subscriber level from/to the core network independently of the access network, maximum security is achieved. The ~~and~~ access network (responsible for the encryption) and the ~~-and~~ core network or networks (responsible for authentication) nonetheless remain functionally separate.

IN 6 A67